4/7/06

Terms used **stream cipher variable sized block** Found **929** of **173,942**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 How to break Gifford's cipher (extended abstract)

Thomas R. Cain, Alan T. Sherman

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.14 MB) Additional Information: full citation, references, index terms

Keywords: Boston Community Information System, Gifford's cipher, algorithms over finite fields, correlation attack, cryptanalysis, cryptography, cryptology, filter generators, linear algebra over GF(2), linear feedback shift registers, matrix decompositions, primary rational canonical form, similar matrices, similarity transformations, stream ciphers

2 Programming by sketching for bit-streaming programs

Armando Solar-Lezama, Rodric Rabbah, Rastislav Bodík, Kemal Ebcioğlu

June 2005 **ACM SIGPLAN Notices , Proceedings of the 2005 ACM SIGPLAN conference on Programming language design and implementation PLDI '05**, Volume 40 Issue 6

Publisher: ACM Press

Full text available: pdf(320.08 KB) Additional Information: full citation, abstract, references, index terms

This paper introduces the concept of *programming with sketches*, an approach for the rapid development of high-performance applications. This approach allows a programmer to write clean and portable reference code, and then obtain a high-quality implementation by simply *sketching* the outlines of the desired implementation. Subsequently, a compiler automatically fills in the missing details while also ensuring that a completed sketch is faithful to the input reference code. In this p ...

Keywords: StreamIt, domain specific compiler, domain specific language, sketching, stream programming, synchronous dataflow

3 The use of cryptography to create data file security: with the Rijndael cipher block

John D. Haney

February 2006 **Journal of Computing Sciences in Colleges**, Volume 21 Issue 3

Publisher: Consortium for Computing Sciences in Colleges

Full text available: pdf(195.83 KB) Additional Information: full citation, abstract, references, index terms

The use of cryptography, both the encryption and decryption of data is one response to the concerns of securing data files. The Rijndael cipher block, which has been adopted by the National Institute of Standards and technology as the advanced encryption standard, has been used in this study to encrypt and decrypt data. This has been accomplished by encrypting a plain text file and creating an encrypted file in one program, and decrypting the encrypted file back to a plain text file in another p ...

4 OCB: A block-cipher mode of operation for efficient authenticated encryption

Phillip Rogaway, Mihir Bellare, John Black

August 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 3

Publisher: ACM Press

Full text available: pdf(568.74 KB) Additional Information: full citation, abstract, references, index terms

We describe a parallelizable block-cipher mode of operation that simultaneously provides privacy and authenticity. OCB encrypts-and-authenticates a nonempty string *M* ∈ {0, 1}* using □&vertbar;*M*&vertbar;/*n*□ + 2 block-cipher invocations, where *n* is the block length of the underlying block cipher. Additional overhead is small. OCB refines a scheme, IAPM, suggested by Charanjit Jutla. Desirable properties of OCB include the ability to encrypt a bi ...

Keywords: AES, authenticity, block-cipher usage, cryptography, encryption, integrity, modes of operation, provable security, standards

5 Reception and posters: Securing media for adaptive streaming

Chitra Venkatramani, Peter Westerink, Olivier Verscheure, Pascal Frossard

November 2003 **Proceedings of the eleventh ACM international conference on Multimedia**

Publisher: ACM Press

Full text available: pdf(233.56 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes the ARMS system which enables secure and adaptive rich media streaming to a large-scale, heterogeneous client population. The secure streaming algorithms ensure end-to-end security while the content is adapted and streamed via intermediate, potentially untrusted servers. ARMS streaming is completely standards compliant and to our knowledge is the first such end-to-end MPEG-4-based system.

Keywords: MPEG-4, adaptive, encrypted, scalability, streaming, video server

6 Security Mechanisms in High-Level Network Protocols

Victor L. Voydock, Stephen T. Kent

June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2

Publisher: ACM Press

Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

7 Low power scalable encryption for wireless systems

James Goodman, Anantha P. Chandrakasan

January 1998 **Wireless Networks**, Volume 4 Issue 1

Publisher: Kluwer Academic Publishers

Full text available: pdf(7.39 MB) Additional Information: full citation, abstract, references, index terms

Secure transmission of multimedia information (e.g., voice, video, data, etc.) is critical in many wireless network applications. Wireless transmission imposes constraints not found in typical wired systems such as low power consumption, tolerance to high bit error rates, and scalability. A variety of low power techniques have been developed to reduce the power of several encryption algorithms. One key idea involves exploiting the variation in computation requirements to dynamically vary th ...

8 Wireless network security I: Application of synchronous dynamic encryption system in mobile wireless domains

Hamdy S. Soliman, Mohammed Omari

October 2005 **Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks Q2SWinet '05**

Publisher: ACM Press

Full text available: pdf(159.81 KB) Additional Information: full citation, abstract, references, index terms

Motivated by the tradeoff between security and efficiency performance parameters that has been imposed on all modern wireless security protocols, we designed a novel security system that gained in both parameters. Our system is based on stream ciphers for their speed, but maintaining a much more solid and proven security. Such security strength stems from the novel deployment of permutation vectors and the data records in the regeneration of the secret key. Moreover, the involvement of the forme ...

Keywords: dynamic encryption, flexible integrity, integrity violations, mobile network security, permutation vectors, seamless handover

9 Hardware Engines for Bus Encryption: A Survey of Existing Techniques

R. Elbaz, L. Torres, G. Sassatelli, P. Guillemin, C. Anguille, M. Bardouillet, C. Buatois, J. B. Rigaud

March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**

Publisher: IEEE Computer Society

Full text available: pdf(194.68 KB) Additional Information: full citation, abstract

The widening spectrum of applications and services provided by portable and embedded devices bring a new dimension of concerns in security. Most of those embedded systems (pay-TV, PDAs, mobile phones, etc...) make use of external memory. As a result, the main problem is that data and instructions are constantly exchanged between memory (RAM) and CPU in clear form on the bus. This memory may contain confidential data like commercial software or private contents, which either the end-user or the c ...

10 Content analysis: A novel encryption algorithm for high resolution video

Fuwen Liu, Hartmut Koenig

June 2005 **Proceedings of the international workshop on Network and operating systems support for digital audio and video NOSSDAV '05**

Publisher: ACM Press

Full text available: pdf(335.72 KB) Additional Information: full citation, abstract, references, index terms

The popularity of multimedia applications is rapidly growing nowadays. The confidentiality of video communication is of primary concern for their commercial use, e.g. in video on demand services or in multiparty video conferences. Specific video encryption algorithms are strongly required in real-time multimedia communication to fulfill the strict timing requi-rements. In this paper we present a novel video encryption algorithm, called *Puzzle*, to encrypt video data in software. It is fast ...

Keywords: data security, multimedia com-munication, real-time video encryption, video compression

11 Pedagogy: A proposed curriculum of cryptography courses

Wasim A. Al-Hamdani, Ivory J. Griskell

September 2005 **Proceedings of the 2nd annual conference on Information security curriculum development InfoSecCD '05**

Publisher: ACM Press

Full text available: pdf(148.92 KB) Additional Information: full citation, abstract, references, index terms

The Cryptography Course is a major part of Computer security, Information security, Network security and all Information security related courses [12, chapter 1]. This course could be offered to undergraduate level (S level) or graduate level students. This article focuses on the problem:If the Cryptography course is offered as two consecutive courses, there is no problem because there are about 30-32 weeks of instruction for the 3-credit course (about 100 hours). This quantity of time is quite ...

Keywords: curriculum development, curriculum instruction, information assurance, information assurance curriculum, information security, information security curriculum

12 Symmetric and Asymmetric Encryption

Gustavus J. Simmons

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Publisher: ACM Press

Full text available: pdf(2.23 MB) Additional Information: full citation, references, citings, index terms

13 Short papers: Application of synchronous dynamic encryption system (SDES) in wireless sensor networks

Hamdy S. Soliman, Mohammed Omari

October 2005 **Proceedings of the 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks PE-WASUN '05**

Publisher: ACM Press

Full text available: pdf(59.63 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we introduce a novel security protocol for wireless network of sensors. The new security mechanism is efficient, flexible, and very amenable for deployment in the resource constrained sensor networks. Our cryptosystem is a simple and fast stream cipher that utilizes permutation vectors as encryption keys, forcing an intruder to a brute-force time complexity of $\Omega(2^n)$. In addition, our mechanism alleviates the effect of sensor capture, via its re-keying feature. It a ...

Keywords: deployment knowledge, encryption permutation vectors, power balancing, sensors security primitives, stream ciphers

14 Secure password-based cipher suite for TLS

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2

Publisher: ACM Press

Full text available: pdf(507.57 KB) Additional Information: full citation, abstract, references, citings, index terms, review

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the protocol itself seems rather secure, there are a number of risks that lurk in its

use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect forward secrecy, secure channel, transport layer security, weak secret

15 Securing ATM networks

Shaw-Cheng Chuang

January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

16 Network protocols: State based key hop protocol: a lightweight security protocol for wireless networks

Stephen Michell, Kannan Srinivasan

October 2004 **Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks**

Publisher: ACM Press

Full text available: pdf(293.45 KB) Additional Information: full citation, abstract, references, index terms

State Based Key Hop (SBKH) protocol provides a strong, lightweight encryption scheme for battery operated devices, such as the sensors in a wireless sensor network, as well as small office home office (SOHO) users. Although SBKH can be applied to many underlying protocols, in this paper, we focus on integrating SBKH with 802.11. Hence we compare SBKH with other 802.11 security protocols and show that SBKH eliminates all the issues with wired equivalent privacy (WEP) protocol, using the existing ...

Keywords: computer network security, low power security, state based encryption, wireless security, wireless sensor network security

17 Encryption-based protection for interactive user/computer communication

Stephen Thomas Kent

September 1977 **Proceedings of the fifth symposium on Data communications**

Publisher: ACM Press

Full text available: pdf(846.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper develops a virtual connection model, complete with intruder, for interactive terminal-host communication and presents a set of protection goals that characterize the security that can be provided for a physically unsecured connection. Fundamental requirements for protocols that achieve these goals and the role of encryption in the design of such protocols are examined. Functional and security constraints on positioning of protection protocols in a communication system and the imp ...

18 Resource management: A charging and rewarding scheme for packet forwarding in multi-hop cellular networks

Naouel Ben Salem, Levente Buttyán, Jean-Pierre Hubaux, Markus Jakobsson

June 2003 **Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing**

Publisher: ACM Press

Full text available: pdf(225.98 KB) Additional Information: full citation, abstract, references, citings, index terms

In multi-hop cellular networks, data packets have to be relayed hop by hop from a given mobile station to a base station and vice-versa. This means that the mobile stations must accept to forward information for the benefit of other stations. In this paper, we propose an incentive mechanism that is based on a charging/rewarding scheme and that makes collaboration rational for selfish nodes. We base our solution on symmetric cryptography to cope with the limited resources of the mobile stations. ...

Keywords: ad hoc networks, billing, charging, cooperation, hybrid cellular networks, multi-hop cellular networks, packet forwarding, pricing, security

19 Fast implementations of secret-key block ciphers using mixed inner- and outer-round pipelining

Pawel Chodowiec, Po Khuon, Kris Gaj

February 2001 **Proceedings of the 2001 ACM/SIGDA ninth international symposium on Field programmable gate arrays**

Publisher: ACM Press

Full text available: pdf(691.29 KB) Additional Information: full citation, abstract, references, citings, index terms

The new design methodology for secret-key block ciphers, based on introducing an optimum number of pipeline stages inside of a cipher round is presented and evaluated. This methodology is applied to five well-known modern ciphers, Triple DES, Rijndael, RC6, Serpent, and Twofish, with the goal to first obtain the architecture with the optimum throughput to area ratio, and then the architecture with the highest possible throughput. All ciphers are modeled in VHDL, and implemented using Xilinx ...

Keywords: AES, fast architectures, pipelining, secret-key ciphers

20 Security on FPGAs: State-of-the-art implementations and attacks

Thomas Wollinger, Jorge Guajardo, Christof Paar

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3

Publisher: ACM Press

Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

4/7/06

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	4	("20020131591" | "20020150240" | "5245658" | "5991403").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/04/07 14:46
L5	0	(stream adj cipher and (random adj (size length) adj block)).clm.	US-PGPUB; USPAT	OR	ON	2006/04/07 15:28
L6	0	(stream adj cipher and (variable adj (size length) adj block)).clm.	US-PGPUB; USPAT	OR	ON	2006/04/07 15:28
L7	3	(stream adj cipher and (variable adj (sized length) adj block)).clm.	US-PGPUB; USPAT	OR	ON	2006/04/07 15:29
L8	3	(stream adj cipher and ((variable random$2) adj (sized length) adj block)).clm.	US-PGPUB; USPAT	OR	ON	2006/04/07 15:29
L9	4	(stream adj cipher and ((variable random$2) adj (sized length))). clm.	US-PGPUB; USPAT	OR	ON	2006/04/07 15:29
S1	4	(time near10 seed) same cipher	USPAT	OR	OFF	2004/08/03 16:03
S2	14	(time same seed) same cipher	USPAT	OR	OFF	2004/08/03 16:52
S3	47	(time same seed) same encrypt	USPAT	OR	OFF	2004/08/03 16:52
S4	0	hybird adj stream adj cipher	USPAT	OR	OFF	2005/03/18 13:53
S5	90	schlumberger-industries.asn.	USPAT	OR	OFF	2004/07/29 13:27
S6	0	epo055366	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/29 13:27
S7	0	ep055366	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/29 13:28
S8	0	ep0599366	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/29 13:28
S9	0	epo599366	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/29 13:28
S10	10	"599366"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/29 13:30
S11	1	("5727062").PN.	USPAT; USOCR	OR	OFF	2004/07/29 13:32

EAST Search History

S12	16	US-4316055-$.DID. OR US-4613901-$.DID. OR US-4953208-$.DID. OR US-5020106-$.DID. OR US-5195136-$.DID. OR US-5509073-$.DID. OR US-5590194-$.DID. OR US-5621799-$.DID. OR US-5673319-$.DID. OR US-5825879-$.DID. OR US-5852472-$.DID. OR US-5862150-$.DID. OR US-5940509-$.DID. OR US-6005940-$.DID. OR US-6061449-$.DID. OR US-6167136-$.DID.	USPAT	OR	OFF	2004/07/29 13:56
S13	634	(380/28).CCLS.	USPAT; USOCR	OR	OFF	2004/07/29 13:59
S14	211	(380/37).CCLS.	USPAT; USOCR	OR	OFF	2004/07/29 13:59
S15	369	(380/44).CCLS.	USPAT; USOCR	OR	OFF	2004/07/29 13:59
S16	487	(380/46).CCLS.	USPAT; USOCR	OR	OFF	2004/07/29 14:00

EAST Search History

S17	97	("4316055" "4107458" "5724427" "6122379" "5297207" "5724428" "4322576" "5835600" "5703952" "6345101" "5341425" "5696826" "4471164" "5835597" "6069954" "5684876" "6278780" "6064738" "6760440" "5195136" "5428686" "5734721" "4369332" "5742756" "5764766" "5796836" "4868877" "5070528" "5375169" "5787173" "6125185" "5768390" RE30957 "6226742" "6226742" "6128737" "6490354" "5825886" "5761306" "6240187" "4979832" "4078152" "5454039" "5675652" "6249582" "4815130" "6052786" "6192129" "6243470" "5623549").pn. ("6269163" "6570989" "5818934" "4608455" "5016275" "4856063" "5345507" "5671284" "4916738" "6148400" "6697490" "4262329" "6011847" "6108421" "6708893" "6404888" "6101543" "6763363" "4797921" "6560338" "4304961" "4314097" "5504818" "5799090" "6128386" "6628786" "5793871" "6081598" "6173402" "6282295" "5949884" "6182216" "6199162" "4797928" RE35403 "6298136" "6578150" "6751319" "4375579" "5727062" "6393125" "6415032" "4633036" "6278783" "5365591" "6269164" "5481610" "6061449" "6061449").pn.	USPAT	OR	OFF	2004/07/29 14:05
S18	0	(cipher encrypt) and (variable-sized adj block)	USPAT	OR	OFF	2005/03/16 13:46
S19	0	(cipher encrypt) and (variable-sized adj blocks)	USPAT	OR	OFF	2004/07/29 14:05
S20	0	(cipher encrypt) and (variable adj sized adj blocks)	USPAT	OR	OFF	2004/07/29 14:05
S21	0	(cipher encrypt) and (variable-size adj blocks)	USPAT	OR	OFF	2004/07/29 14:06
S22	2	(cipher encrypt) and (variable adj size adj blocks)	USPAT	OR	OFF	2004/07/29 14:07
S23	12	("3798359" | "3798360" | "3962539" | "4078152" | "4157454" | "4275265" | "4316055" | "4751733" | "4979832" | "5003597" | "5214703" | "5231662").PN.	USPAT	OR	OFF	2004/07/29 14:06

EAST Search History

S24	198	(cipher encrypt) and ((variable adj (size sized sizes length)) same (blocks block))	USPAT	OR	OFF	2004/07/29 14:08
S25	15	(cipher encrypt) and ((variable adj (size sized sizes length)) adj (blocks block))	USPAT	OR	OFF	2004/07/29 15:53
S26	11	("4275265" | "5159634" | "5214703" | "5687238" | "5794139" | "5991407" | "6075859" | "6266411" | "6377687" | "6385316" | "6393270").PN.	USPAT	OR	OFF	2004/07/29 14:08
S27	1	("6154541").PN.	USPAT; USOCR	OR	OFF	2004/07/29 15:53
S28	1	("6243470").PN.	USPAT; USOCR	OR	OFF	2004/07/30 15:54
S29	1	collberg.in.	USPAT	OR	OFF	2004/07/30 18:10
S30	6	collberg.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/30 15:57
S31	5	(digital adj watermark) same (random adj data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/30 15:59
S32	24	(watermark) same (random adj data)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/30 16:50
S33	0	"20020085710".URPN.	USPAT	OR	OFF	2004/07/30 16:00
S34	1	("5822432").PN.	USPAT; USOCR	OR	OFF	2004/07/30 16:50
S35	21	(watermark) same (random adj (value values))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/07/30 16:50
S36	2	(mix mixing permute permuting shuffle shuffling combine) same (signature and watermark)	USPAT	OR	OFF	2004/07/30 19:05
S37	87	cipher and (table adj lookup)	USPAT	OR	OFF	2004/07/30 19:05
S38	1	("6243470").PN.	USPAT; USOCR	OR	OFF	2004/08/03 16:01
S39	1	("5892900").PN.	USPAT; USOCR	OR	OFF	2004/08/02 15:58
S40	1	("5727062").PN.	USPAT; USOCR	OR	OFF	2004/08/02 15:59

EAST Search History

S41	12	("3798359" | "3798360" | "3962539" | "4078152" | "4157454" | "4275265" | "4316055" | "4751733" | "4979832" | "5003597" | "5214703" | "5231662").PN.	USPAT	OR	OFF	2004/08/02 16:00
S42	12	"5727062".URPN.	USPAT	OR	OFF	2004/08/02 16:00
S43	50	"5822432"	USPAT	OR	OFF	2004/08/03 14:45
S44	1	("5822432").PN.	USPAT; USOCR	OR	OFF	2004/08/03 14:45
S45	0	(cipher encrypt) and (variable adj sized adj block)	USPAT	OR	OFF	2005/03/16 13:46
S46	9	(cipher encrypt) and (variable adj length adj block)	USPAT	OR	OFF	2005/03/16 13:46
S47	14	(cipher encrypt) and (variable adj length adj block$)	USPAT	OR	OFF	2005/03/16 14:22
S48	166	(380/42).CCLS.	USPAT	OR	OFF	2005/03/16 15:06
S49	1	("6122379").PN.	USPAT	OR	OFF	2005/03/16 16:14
S50	260	(380/43).CCLS.	USPAT	OR	OFF	2005/03/16 16:15
S51	1	S50 and (variable different) adj size	USPAT	OR	OFF	2005/03/16 16:15
S52	18	S50 and (stream adj cipher)	USPAT	OR	OFF	2005/03/16 17:03
S53	21	S48 and (stream adj cipher)	USPAT	OR	OFF	2005/03/16 17:03
S54	1	("6212635").PN.	USPAT	OR	OFF	2005/03/16 17:35
S55	2	encrypt and (internal adj identifier)	USPAT	OR	OFF	2005/03/16 17:35
S56	1	("6212635").PN.	USPAT	OR	OFF	2005/03/17 12:35
S57	1	("6154541").PN.	USPAT	OR	OFF	2005/03/17 12:35
S58	1	("6122379").PN.	USPAT	OR	OFF	2005/03/17 17:00
S59	1007	((380/37) or (380/44) or (380/46)).CCLS.	USPAT	OR	OFF	2005/03/17 17:00
S60	40	S59 and (@pd > "20040802")	USPAT	OR	OFF	2005/03/17 17:01
S61	1337	((380/37) or (380/42) or (380/43) or (380/44) or (380/46)).CCLS.	USPAT	OR	OFF	2005/11/16 21:05
S62	81	S61 and (@pd > "20050318")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 10:45
S63	256	(380/37).CCLS.	USPAT	OR	OFF	2005/11/18 10:46
S64	1	("6122379").PN.	USPAT	OR	OFF	2005/11/18 11:21

EAST Search History

S65	881	(initialization adj vector)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:19
S66	589	(initialization adj vector) same (encrypt$)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:20
S67	0	(initialization adj vector) and (encrypt$) and (variable random) adj (sized adj block)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:20
S68	1	(seed) and (encrypt$) and (variable random) adj (sized adj block)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:21
S69	4	(seed) and (encrypt$) and (variable random) adj (length adj block)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:23
S70	273	(seed) and (encrypt$) and (variable random) with ((size length) near10 block)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:23
S71	184	(seed) and (encrypt$) same (variable random) with ((size length) near10 block)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:32
S72	0	(seed) and (encrypt$) same (variable random) with ((size length) near10 block) and 7??/*.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:33

EAST Search History

S73	67	(seed) and (encrypt$) same (variable random) with ((size length) near10 block) and 7??/$. ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/18 12:52
S74	1	("6490353").PN.	USPAT	OR	OFF	2005/11/18 12:52
S75	8	("4736423" | "5245658" | "5247576" | "5548648" | "5619576" | "5659614" | "5835600" | "6182216").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2005/11/18 12:52
S76	2	("6490353").URPN.	USPAT	OR	ON	2005/11/18 12:55
S78	4	("4815130" | "5720034" | "5764766" | "6445794").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2005/11/18 12:57
S79	1409	((380/37) or (380/42) or (380/43) or (380/44) or (380/46)).CCLS.	USPAT	OR	OFF	2006/04/05 19:11
S80	71	S79 and (@pd > "20051118")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/04/07 14:45
S81	1	("7003107").PN.	USPAT	OR	OFF	2006/04/07 15:26